Manual del usuario

Versión: 1.1
Fecha: Octubre 2010

www.SEGO.com.pe

Acerca de este documento:
Este documento presenta las operaciones del dispositivo de control de acceso. Para la instalación del producto, consulte la guía de instalación correspondiente. Para el software funcionamiento, consulte el manual de usuario del software.

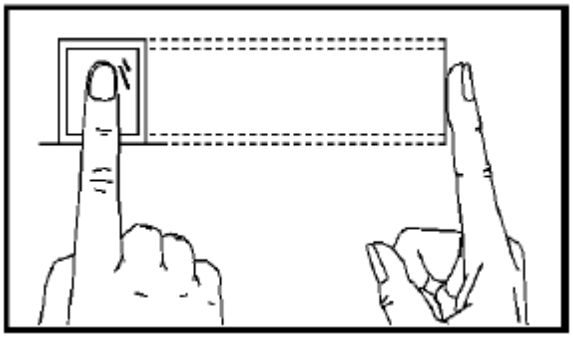
1. Instrucciones para el uso:

1.1 Colocación de los dedos:

Dedos recomendados: *el dedo índice, dedo medio o en el dedo anular.*

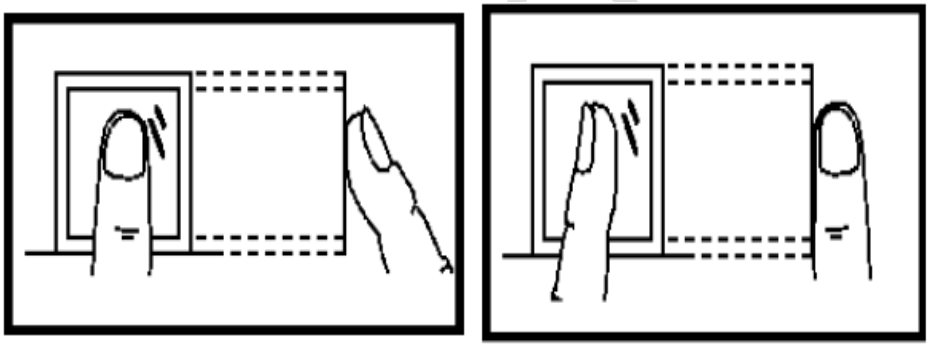
Dedos no recomendados: *el pulgar y el meñique no se recomiendan (ya que suelen ser torpes en la pantalla al momento de marcar la huella dactilar).*

- **Adecuada colocación del dedo:**

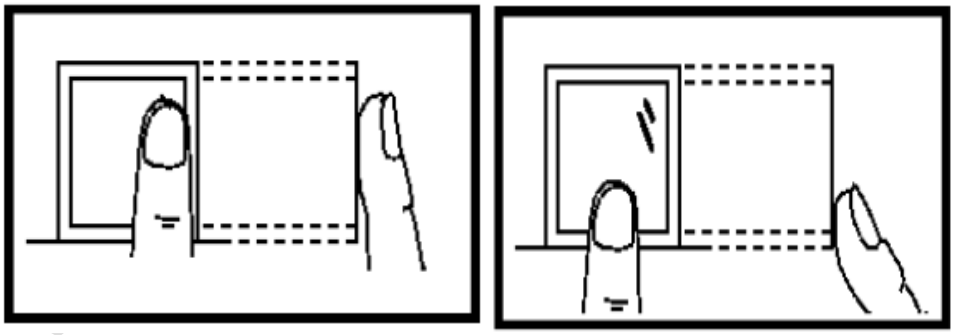


Colocar el dedo en forma plana y centrada en la lectora de huella

- **Incorrecta colocación de los dedos:**
  - *Inclinación:*



  - *Descentrado:*



1.2 Instrucciones para la tarjeta magnética:

Lector de tarjetas integrado con un modulo no-contacto RF, este dispositivo es compatible con las tarjetas de identificación y tarjetas Mifare **(opcional)** *y sólo se utilizan como tarjetas de*

identificación. Al ofrecer múltiples modos de verificación tales como huellas digitales, tarjeta de RF y de verificación de huella digital + tarjeta RF, este dispositivo puede adaptarse a las necesidades diversificadas del usuario.

Deslice su tarjeta en el área del sensor después de que el mensaje de voz y retirar la tarjeta después de que el dispositivo lo ha detectado. Por la zona de deslizamiento, véase el punto 2.2 el aspecto del producto.

1.3 Precauciones

Proteja el aparato de la exposición a la luz solar directa ó fuerte luz, ya que un fuerte rayo de luz afecta en gran medida el reconocimiento de huellas dactilares y conduce al fracaso verificación de huellas dactilares.

Se recomienda utilizar el dispositivo bajo una temperatura de 0-50°C a fin de lograr el rendimiento óptimo. En el caso de la exposición del dispositivo a la intemperie durante largos períodos de tiempo, se recomienda adoptar parasol y las instalaciones de disipación de calor debido a temperatura demasiado alta o demasiado baja puede lentizar el funcionamiento del dispositivo y en consecuencia alta tasa de falso rechazo (TRF) y tasa de falsa aceptación (FAR).

Al instalar el aparato, por favor conecte el cable de alimentación antes de conectar cualquier otro cable. Si el dispositivo no funciona correctamente, asegúrese de apagar la fuente de alimentación antes de realizar la inspección necesaria. Tenga en cuenta que cualquier trabajo con el equipo encendido puede causar daños en el dispositivo y los daños que surjan después de trabajar el equipo encendido queda fuera del alcance de la garantía normal. Respecto de los asuntos que no están cubiertos en este documento, por favor refiérase a los materiales relacionados, incluyendo la guía de instalación, software de control de acceso manual de usuario.

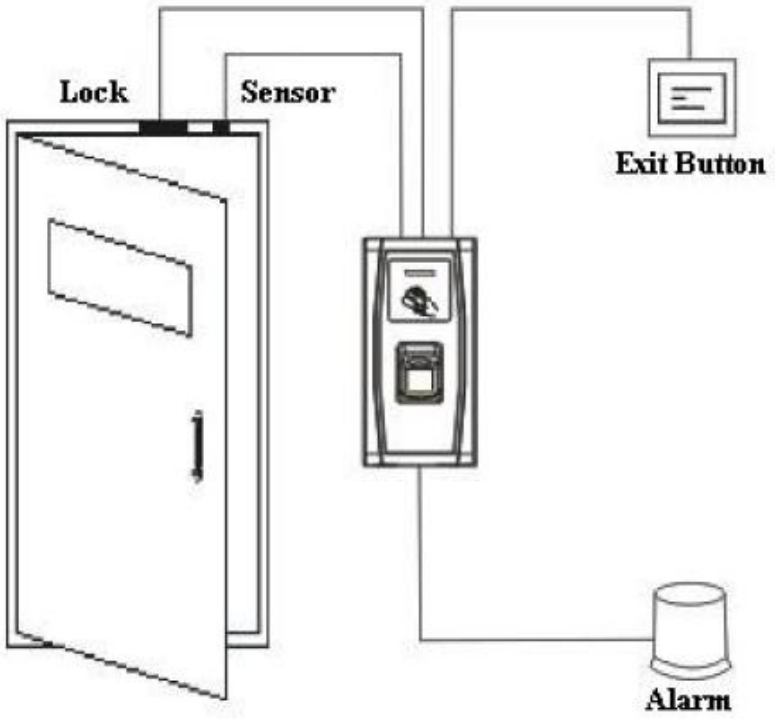
2. La introducción de dispositivos:

2.1 Resumen de las funciones del dispositivo:

Como un equipo de huellas y control de acceso integrado, nuestro producto se puede conectarse con cualquier cerradura electrónica o controlador de acceso. Este dispositivo cuenta con operaciones sencillas y flexibles, y apoya el uso de tarjetas de administración. Con una tarjeta de gestión, se pueden realizar funciones tales como la inscripción en línea, eliminación y gestión de U-disco. La voz le guiará a través de todas las operaciones sin pantalla. Este dispositivo le permite conectar un teclado externo USB y ofrece múltiples modos de operación.

Es compatible con la función de control de acceso para una gestión de la seguridad. Es compatible con varios modos de comunicación. El U-disco cuenta con operaciones simples y convenientes. El diseño resistente al agua y caja de metal del dispositivo le permite soportar un fuerte impacto sin sufrir daños. Con un diseño compacto y simple, este dispositivo permite a los usuarios conectar varios dispositivos a través de una PC y realizar seguimiento en tiempo real de los accesos.

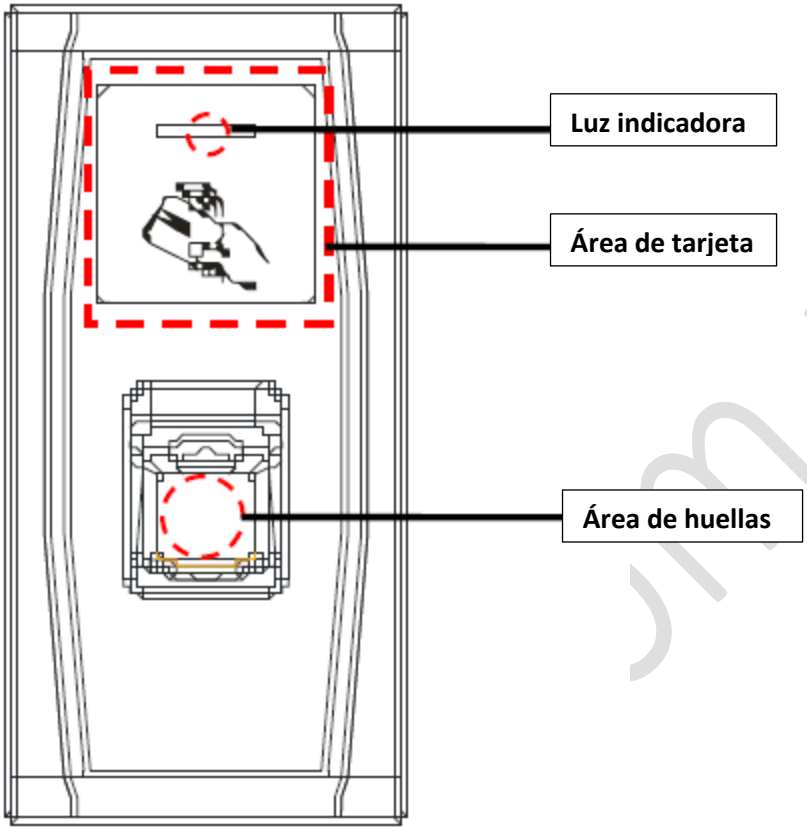
www.SEGO.com.pe



2.2 Apariencia del producto:

Vista frontal:

www.SEGO.com.pe



Indicador LED: *el indicador LED se utiliza para mostrar el funcionamiento del dispositivo y el resultado de estados excepcionales los cuales se definen de la siguiente manera:*

Reglas comunes*: si la operación tiene éxito, la luz del indicador verde es sólida en un segundo, de lo contrario, el indicador rojo es sólida por un segundo.*

Estado de matrícula: *el LED verde parpadea tres veces por otros tres segundos.*

La supresión de Usuario único: *el LED parpadea tres veces cada dos tres segundos*

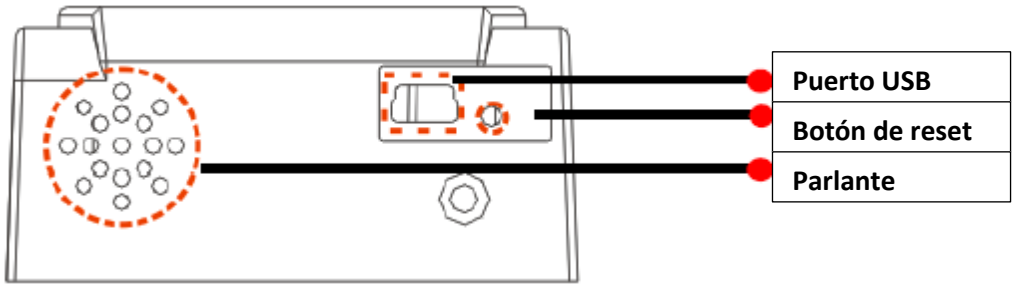
Estado de verificación: *el LED verde parpadee una vez por otros dos segundos.*

Tarjeta de la zona de paso: *se refiere a la zona en la discontinua de color rojo - caja de línea como se muestra en la figura anterior.*

Sensor de huellas digitales: *se utiliza para recopilar y comparar huellas y eliminar usuarios.*

Vista desde abajo:

www.SEGO.com.pe

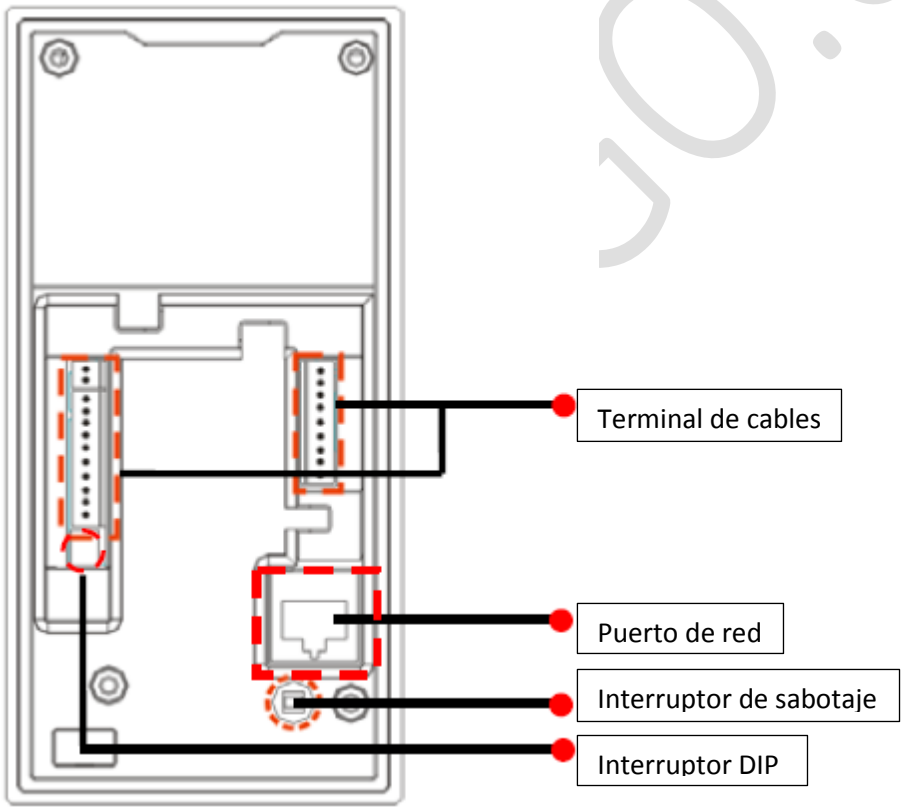


Interfaz USB: *se utiliza para conectar con un U-disco ó un teclado externo USB.*

El botón de reinicio: *se utiliza para reiniciar el dispositivo*

Altavoces: *se utiliza para reproducir el sonido de pitido y de voz. Si un usuario esta agregado en la lectora el altavoz emite un pitido, si un usuario no esta agregado en la lectora emite dos veces pitidos. El valor por defecto pedirá durante la operación:* **Señal + voz sonora.**

Vista trasera:



Terminal de cables: *se conecta con las cerraduras y el suministro de energía a través de los cables.*

TCP / IP de la interfaz: *la interfaz de TCP / IP se conecta con una PC mediante un cable de red (para la conexión detallada, consulte la guía de instalación).*

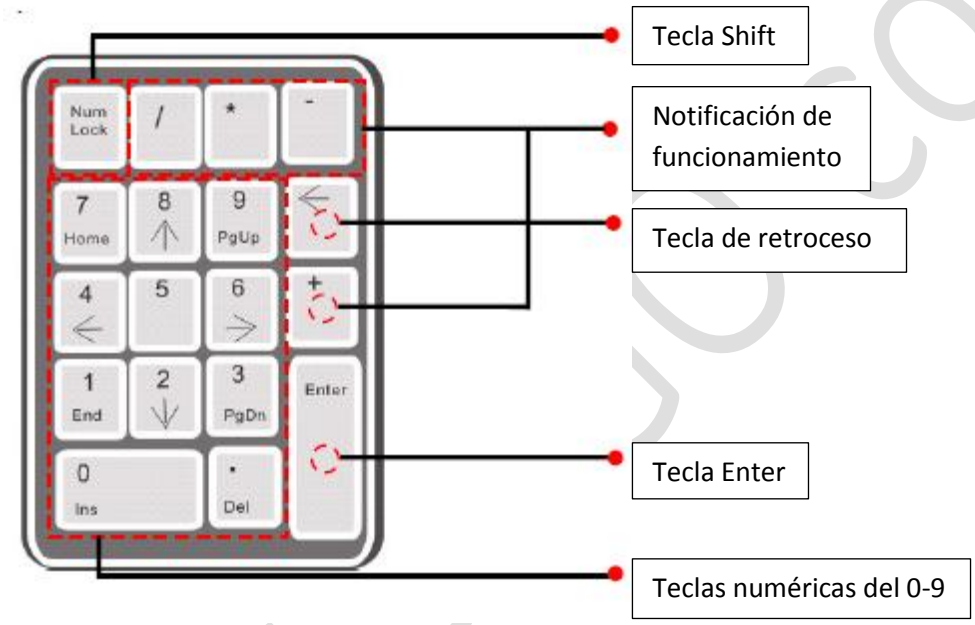
Interruptor de sabotaje: *se utiliza para generar una alarma de sabotaje. Para más detalles, véase el apartado 3.6 del interruptor de sabotaje.*

Interruptor DIP: *el interruptor DIP tiene cuatro pines numerados 1, 2, 3 y 4.*

En el modo de comunicación RS 485, los pines a usar son **1, 2** *y* **3** *se utilizan para fijar el número de dispositivo de hardware y el cuarto pin se utiliza para seleccionar el estado de resistencia terminal. Para la configuración detallada, consulte la guía de instalación.*

2.3 Uso de un teclado USB externo

Para facilitar las operaciones del dispositivos, puede conectarse a él con un teclado externo USB (adquirido por los usuarios) y llevar a cabo operaciones tales como la inclusión del usuario, la eliminación y restauración de los valores de fábrica, sobre todo cuando se especifica los ID de usuario durante la inscripción y eliminación del usuario.



Arriba se muestra un teclado USB externo **(consulte el producto real)**

Bloq Num: *es un botón del teclado numérico. Se activa por defecto. Si se activa, el indicador LED está activado. Cuando el dispositivo está conectado con un teclado externo, sólo puede usar las teclas numéricas, o retroceder clave e introducir clave en el estado de Bloq Num activado.*

2.4 Verificacion de estado:

Verificacion de estado: *Después de que el dispositivo esté encendido. El dispositivo entra en el estado de verificación si se han inscrito ó inscrito correctamente una tarjeta de administración ó en caso de tiempo de espera de cualquier operación.*

En el estado de verificación, todos los usuarios se les permite verificar su identidad y desbloquear (el administrador teniendo una tarjeta de administración sólo puede desbloquear usando su huella

dactilar matriculado anteriormente); el administrador puede realizar estas operaciones como inscripción de usuario / eliminación, U disco operación administración y teclado.

2.5 Gestión de tarjetas

Los usuarios del dispositivo se clasifican en administrador y los usuarios normales.

Administradores: *un administrador puede realizar todas las operaciones, incluyendo la inscripción de usuario / eliminación (borrar todo los datos de los usuarios) y administración de discos U. Los privilegios de los administradores de dispositivo son implementar a través de la tarjeta de gestión.*

Una tarjeta de administración: *es una tarjeta especialmente asignada para un súper administrador. Cada dispositivo debe inscribir al menos una tarjeta de administración. Si no hay tarjeta de administración inscrita, no puede realizar ninguna operación y el sistema generará un mensaje de voz "por favor registrar la tarjeta de administración".*

Puede implementar diferentes funciones por pasar una tarjeta de administración diferentes veces en una fila:

1. *Ningún disco u o teclado externo estén conectados:*
   - *Al pasar la tarjeta de administración una vez, usted puede entrar en estado de inscripción de usuario único.*
   - *Al pasar la tarjeta de administración cinco veces en una fila, puede especificar el estado de eliminación de un solo usuario.*
2. *U disco está conectado:*
   - *Al pasar la tarjeta de administración una vez, puede ir al estado de la administración de disco U.*
3. *Un teclado externo está conectado:*
   - *Al pasar la tarjeta de administración una vez, puede activar el teclado externo.*

Pase consecutivo: *pase consecutivo el intervalo entre dos manotazos en una fila es menos de 5 segundos.*

Las tarjetas de administración pueden eliminarse a través de la función "Borrar todo" del teclado ó sus privilegios de administración liberado a través de software antes de que se eliminen como tarjetas de identificación común. Para obtener más detalles, véase la inscripción de software o teclado de control de acceso.

Un dispositivo sin tarjeta de administración, si tiene la contraseña de teclado, puede activar el externo teclado e inscribirse ó eliminar usuarios.

Nota: *los usuarios que tienen tarjetas de administración sólo pueden verificar su identidad y desbloquear usando sus huellas dactilares matriculados anteriormente.*

2.6 Contraseña del sistema

www.SEGO.com.pe

Una contraseña del sistema es la contraseña que se utiliza para mejorar la seguridad de los datos del dispositivo en TCP / IP o RS485 comunicaciones.

Nota: *la contraseña del sistema puede modificarse mediante el software de control de acceso. Para obtener detalles, consulte el manual de usuario del software de control de acceso.*

2.7 Operación de tiempo de espera

El tiempo de espera del funcionamiento por defecto es 30 segundos. Al inscribir a una tarjeta de administración, eliminar ó inscribir un usuario (incluso en los Estados de la eliminación de participación y uso del teclado externo), el sistema automáticamente le solicitará cada otro 10 segundo si hay en ninguna operación y vuelve al estado de verificación tras solicitándole tres veces. La voz es "tiempo de espera de la operación. El sistema vuelve al estado de verificación"

Nota: *puede configurar el tiempo de espera a través del software de control de acceso.*

3. Operación del dispositivo

3.1 Gestión de tarjeta

3.1.1 Inscribir a una tarjeta de gestión

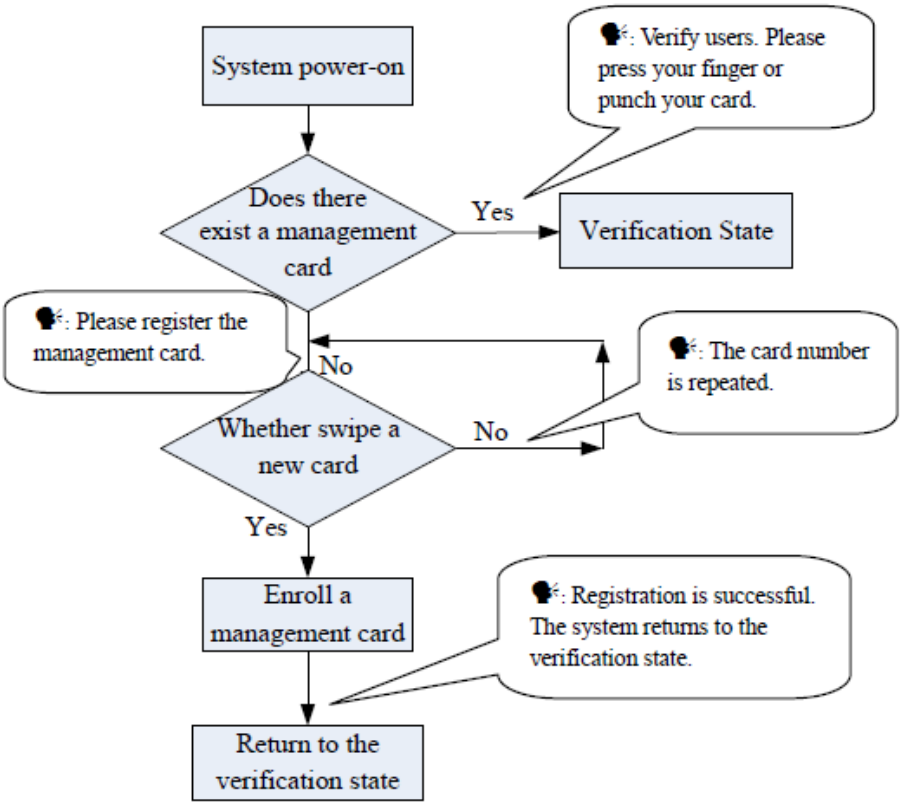
Para inscribir una tarjeta de administración, proceder de la siguiente manera:

1. *El dispositivo detecta automáticamente si existe una tarjeta de administración y entra en el estado de matrícula de la tarjeta de administración. Luego proceda con el paso 3; de lo contrario el sistema genera el mensaje de voz "verificar los usuarios por favor coloque su dedo ó su tarjeta".*

   Nota: *el sistema vuelve al estado verificacion por el tiempo de espera si no se ha realizado ninguna operación en el paso 3 y sólo le pide inscribir a la tarjeta de administración después de resetear el dispositivo nuevamente.*

La tarjeta de gestión del flujo de la inscripción es el siguiente:

www.SEGO.com.pe



3.1.2 inscribir un usuario ordinario

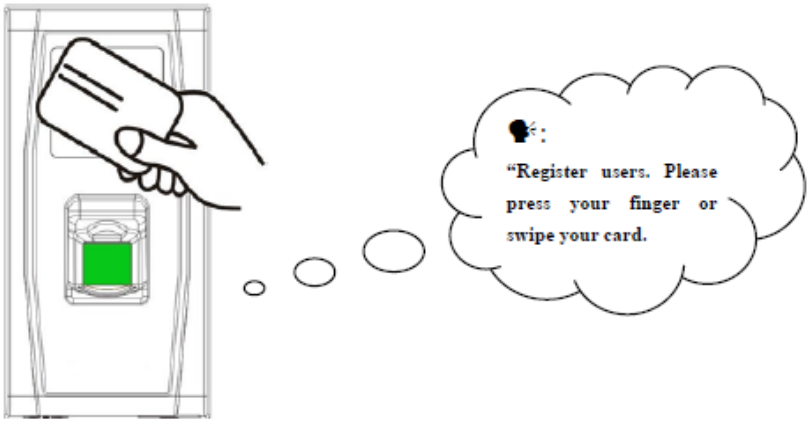
El modo para entrar en el estado de inscripción usando la tarjeta de administración se conoce como la gestión tarjeta ó modo inscripción. En este modo, sólo puede inscribirse un usuario. Cuando se inscriba a un nuevo usuario, el sistema automáticamente definiremos un ID de actividad mínimo para el usuario. Además, también podrá utilizar el modo de inscripción de teclado externo para implementar la inscripción del usuario de ID especificado.

En ambos modos en estas dos inscripciones, se puede inscribir nuevos usuarios. Cada usuario puede inscribirse como máximo 10 huellas digitales y un ID.

Para inscribir a un usuario, haga lo siguiente:

1. *En el estado de verificación, el sistema entra en el estado de inscripción de usuario normal después de que usted pase su tarjeta de administración una vez (en el estado de inscripción, pasar una tarjeta de administración una vez volverá al estado de verificación)*

   Después el sistema genera el mensaje de voz : "registrar usuarios. Por favor coloque su dedo o pase su tarjeta", puede iniciar inscripción del usuario. Existen los siguientes dos casos:



(1) Deslice la tarjeta de ID primero

a. *Cuando usted pase su nueva tarjeta de identificación y realice la inscripción de un usuario, el dispositivo genera un mensaje de voz "número de usuario **. El registro es exitoso!" (** se refiere a la identificación asignada automáticamente al usuario por el sistema) y puede continuar el paso b; Si usted paso una tarjeta de identificación inscrita, el sistema genera un mensaje de voz "usuario número **, presione por favor su dedo!" y entrar en el estado de inscripción de usuario especificado.*
b. *Después de que el dispositivo genera el mensaje de voz "registro". Por favor presione el dedo sobre el sensor tres veces siguiendo las indicaciones de voz.*
c. *Si se logra la inscripción de huellas digitales, el sistema genera el mensaje de voz "el registro es exitoso. Registrar por favor presione el dedo" y entra directamente en el siguiente estado de inscripción de huellas dactilares; Si se produce un error en la inscripción de huellas digitales, el sistema genera el mensaje de voz "la huella repetida" y repite el paso b.*
d. *El sistema vuelve automáticamente al estado de verificación cuando están inscritos 10 dedos y tarjeta de identificación, o la tarjeta de administración es deslizar una vez o agota el tiempo de operación.*

(2) Presione el dedo índice

a. *Pulse el mismo dedo sobre el sensor tres veces siguiendo las indicaciones de voz mediante la adopción de la colocación de la huella correcta. Si se logra la inscripción de huellas digitales, el sistema genera el mensaje de voz "número de usuario **. El registro es exitoso" y puede proceder al paso b; Si va a matricular otra huella de usuario nuevo, el sistema genera el mensaje*

*de voz "número de usuario **, registrarse, por favor presione el dedo o pase tu tarjeta" y entra en el estado de inscripción de usuario especificado.*

b. *Después de generar el mensaje de voz "registrar. Por favor presione el dedo o pase su tarjeta", el sistema entra en el estado de inscripción de información de usuario especificado, espera por le pase a su nuevo ID o que presione el dedo.*
c. *Si la inscripción de la tarjeta de identificación se realiza correctamente, el sistema genera el mensaje de voz "el registro es exitoso. Por favor presione el dedo" y entra en el próximo estado de participación de huellas dactilares; Si presiona un dedo que no está inscrito antes y logra inscripción de dedo, el sistema genera el mensaje de voz "el registro es exitoso. Por favor presione el dedo o pase su tarjeta" y puede seguir inscribiendo nuevas huellas dactilares y tarjetas. Después de inscribirse 10 huellas digitales, el sistema generará el mensaje de voz "por favor perforar su tarjeta" inscribir su tarjeta de identificación si no está inscrito su tarjeta de identificación.*
d. *El sistema vuelve automáticamente al estado de verificación cuando están inscritos 10 dedos y tarjeta de identificación, o la tarjeta de administración es deslizar una vez o agota el tiempo de operación.*

3. Si ya está asignada con un número de usuario, luego están los dos casos siguientes:

(1) Inscripción de huellas dactilar (s) cuando ya se ha inscrito la tarjeta.

*a. Después de pasar la tarjeta de inscripción, el sistema generará el mensaje de voz " número de usuario. ** Regístrate. Por favor, presione su dedo "(** se refiere a la identificación asignada a usted, por debajo de lo mismo) y entrar en el estado de inscripción de huellas dactilares.*

*b. Presione el mismo dedo sobre el sensor tres veces después de las indicaciones de voz mediante la adopción de la colocación de huellas dactilares apropiado. Si la inscripción de huellas dactilares tiene éxito, el sistema genera el mensaje de voz "usuario número **. El registro es exitoso " y se prepara para la inscripción de la huella digital que viene.*
c. El sistema regresa automáticamente al estado de verificación cuando los 10 dedos y tarjeta de identificación está inscrito, o la tarjeta de administración se robó una vez o la operación el tiempo de espera se agotó.

Nota:
1) Si el usuario registrar una huella digital que es la repetición de su propia huella digital inscrito, la nueva huella se sobrepone a la huella digital previamente inscrito.

2) En este modo, la huella digital del usuario que tiene la tarjeta de gestión no puede ser inscrito debido a deslizar la tarjeta de gestión que el sistema vuelva al estado de verificación de forma automática.

www.SEGO.com.pe

(2) Inscripción de tarjetas y huellas digitales (s) cuando ya la huella digital.

a. Presione con el dedo la huella digital a inscrito en tres ocasiones a raíz de la voz. Si se identifican como la misma persona en cada uno de intento de verificación, el sistema entra en estado de inscripción de huellas dactilares.

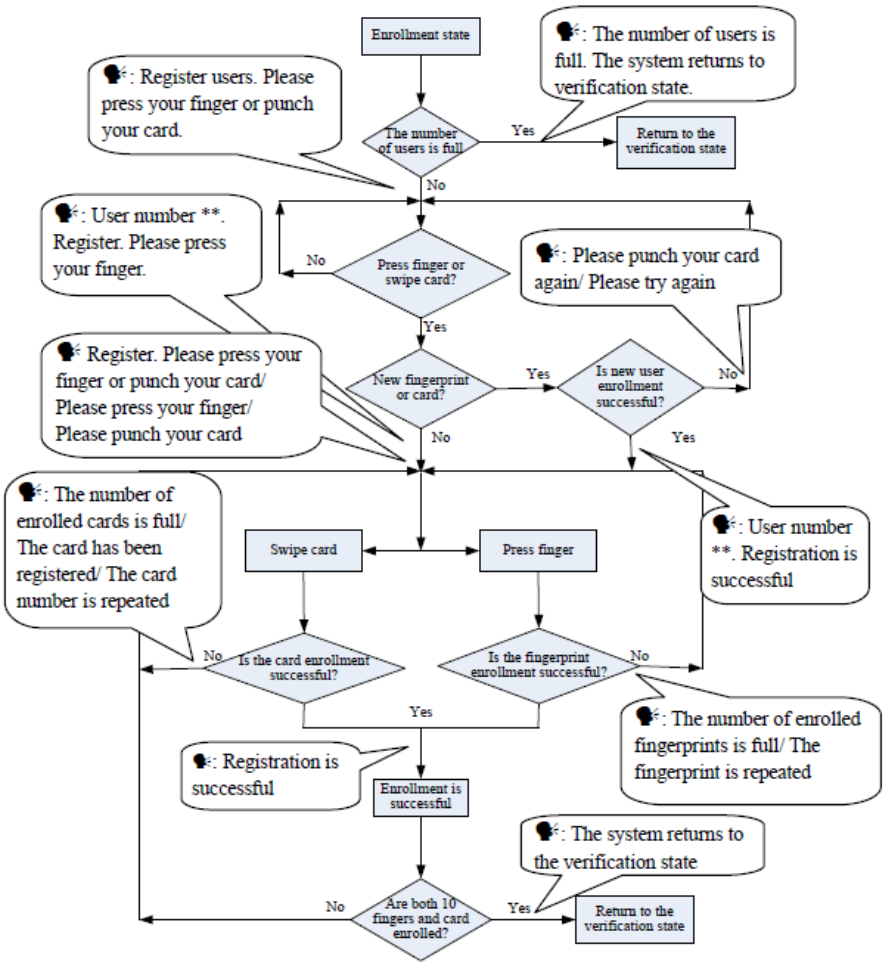
*b. Después de generar el mensaje de voz "el número de usuario. ** Regístrate. Por favor, pulse el dedo o pase su tarjeta ", el sistema comienza a registrar sus huellas digitales.*

c. Si la inscripción tarjeta de identificación tiene éxito, el sistema genera el mensaje de voz "El registro es exitoso. Regístrate. Por favor, presione su dedo "y entra en el estado de inscripción de huellas dactilares directamente, si se presiona con un dedo que no está inscrito antes y tiene éxito en la matrícula de este dedo, el sistema genera el mensaje de voz" El registro es exitoso. Por favor, pulse el dedo o pase su tarjeta" y usted puede seguir las huellas digitales y tarjetas de inscripción de nuevos usuarios. Después de inscribirse 10 huellas dactilares, el sistema generará el mensaje de voz "Por favor, pase su tarjeta" inscribir a su tarjeta de identificación si su tarjeta de identificación no está inscrito.

d. El sistema regresa automáticamente al estado de verificación cuando ambos 10 dedos y tarjeta de identificación está inscrito, o la tarjeta de administración se robó una vez o la operación el tiempo de espera.

El diagrama de flujo que se muestra a continuación:

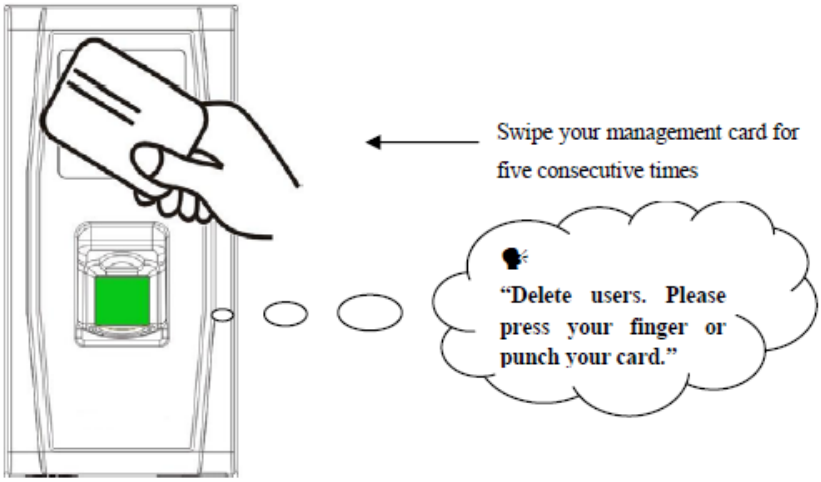
www.SEGO.com.pe



3.1.3 Eliminar un solo usuario

Eliminación de un usuario mediante el uso de una tarjeta de administración.
Los pasos a seguir para la eliminación de un solo usuario:

1. En la verificación del estado, pasa su tarjeta de gestión por cinco veces consecutivas para entrar en el simple estado de monousuario eliminación (pasar la tarjeta una vez más para volver al estado de verificación).



2. El sistema generará el mensaje de voz "Eliminar usuarios. Por favor, pulse el dedo o pase su tarjeta. "

3. Presione su dedo sobre el sensor de huellas digitales o pase su tarjeta por el lector de tarjetas.

(1) Presione su dedo sobre el sensor para eliminar un usuario.
*Pulse uno de sus dedos registrados correctamente en el sensor. Si la verificación tiene éxito, el sistema generará el mensaje de voz "el número de usuario. ** La eliminación se realiza correctamente. usuario eliminado. Por favor, pulse el dedo o pase su tarjeta. "(** Indica el número de identificación del usuario) y automáticamente volverá al estado de borrado. Si la verificación falla, el sistema generará el mensaje de voz "Por favor, inténtelo de nuevo."*

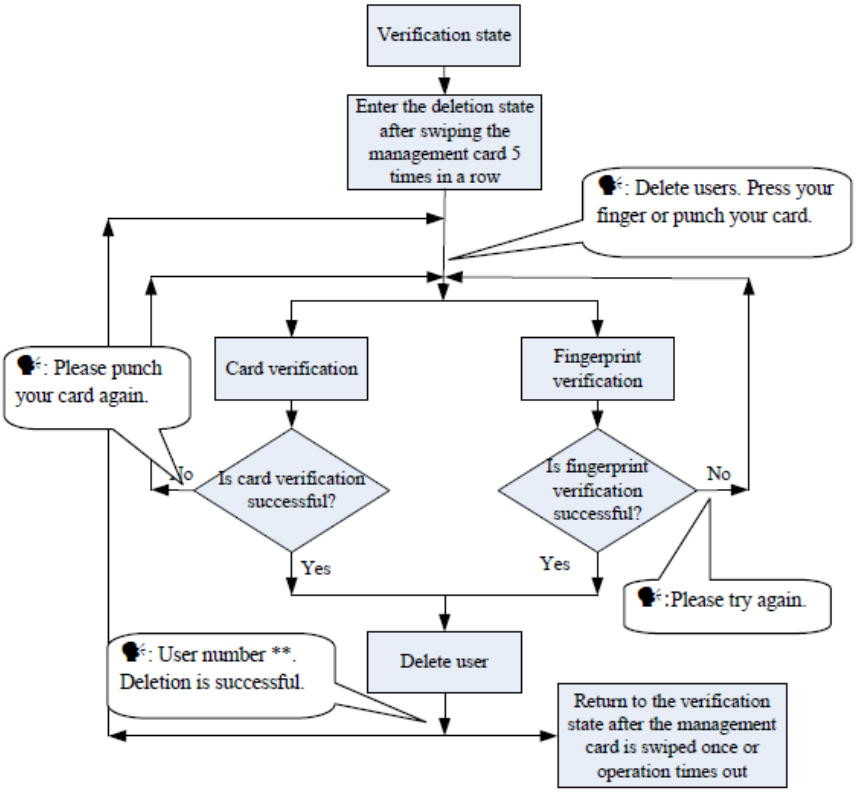
(2) Pase su tarjeta por el lector para eliminar un usuario.
*Pase una tarjeta registrada en el lector. Si la verificación tiene éxito, el sistema generará el mensaje de voz "el número de usuario. ** La eliminación se realiza correctamente. Eliminar usuarios. Por favor, presione su dedo o pase su tarjeta. "Y automáticamente volverá al estado de borrado. Si la verificación falla, el sistema generará el mensaje de voz "Por favor, pase su tarjeta de nuevo."*

4. Si desliza su tarjeta de gestión una vez más, o los tiempos de espera de la operación, el sistema volverá al estado de verificación.

Nota: *En el modo simple eliminación de un solo usuario, los usuarios de gestión de la tarjeta no se puede eliminar porque deslizar la tarjeta de gestión que el sistema vuelva al estado de verificación.*

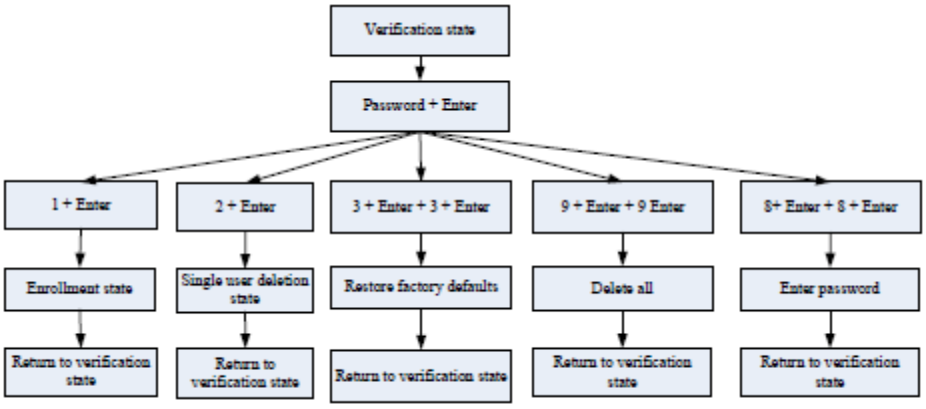
Procedimiento simple para la eliminación de un solo usuario:

www.SEGO.com.pe



3.2 Operaciones del teclado USB

El gráfico de teclado operaciones de flujo se muestra a continuación:



3.2.1 Establecer contraseña de teclado

Si el usuario necesita un teclado externo, él / ella puede conectar el teclado al dispositivo y luego pasar la tarjeta de gestión para activar el teclado externo.
El sistema permite al usuario establecer una contraseña específica para el teclado externo.

Los pasos de la operación:

1. En el estado de verificación, conectar un teclado externo con el dispositivo a través de la interfaz USB.

2. Deslice su tarjeta de gestión de una vez para activar el teclado. El sistema genera el mensaje de voz "Por favor, pulse en el teclado."

3. El tipo de "8" y pulse Enter. A continuación, escriba en "8" y pulse Enter de nuevo. El sistema genera el mensaje de voz "Por favor, establecer contraseña". Escriba la contraseña que desee y pulse Enter. El sistema genera el mensaje de voz "La operación se realiza correctamente. El sistema vuelve a estado de verificación. "Si no hay pulsaciones en 30 segundos, el sistema generará el mensaje de voz " tiempo de espera de la operación. El sistema vuelve al estado de verificación. "(La contraseña debe tener entre 4 y 6 dígitos.)

El usuario puede introducir la contraseña para activar las funciones del teclado externo en el siguiente uso, o pasar una tarjeta de gestión de una vez (que es obligatorio para el primer uso del teclado externo).

1. Si ingresa una contraseña incorrecta por seis veces consecutivas, el teclado se bloqueará y tendrá el poner un nuevo teclado para desbloquear.

2. Si no hay golpes de teclado dentro de los 3 segundos después de que el teclado está activado, las funciones del teclado se desactiva automáticamente y usted tendrá que reactivarla.
3. el teclado se debe inserta o se quita en un intervalo de más de 15 segundos, de lo contrario el sistema no puede identificar su estado.

3.2.2 Inscribir a un usuario a través del teclado

Inscribir a un usuario mediante un teclado USB. En este modo, el usuario puede inscribir a un usuario con el ID de usuario especificado.

Los pasos de la operación:
1. Como se muestra en el punto 3.2 del teclado USB de Operaciones de diagrama de flujo, el tipo de "1" y pulse Enter para entrar en el estado de inscripción.

2. Cuando el sistema genera el mensaje de voz "los usuarios del Registro. Por favor introduce el número de usuario. ", Escriba un ID de usuario.

*3. El sistema genera el mensaje de voz " numero de usuario **. Registrar a los usuarios. Por favor, pulse el dedo o pase su tarjeta. "(** Indica el ID número del usuario, por debajo de lo mismo) El sistema entra en la identificación del estado de inscripción especificado.*

Nota:

*(1) Si un usuario se ha inscrito en el sistema con una tarjeta de gestión, el sistema generará el mensaje de voz "número de usuario. ** Por favor, presione su dedo. "*
*(2) Si un usuario se ha inscrito en el sistema con un ID de usuario y las huellas digitales de 10, el sistema generará el mensaje de voz "número de usuario. ** Por favor pase su tarjeta. "*

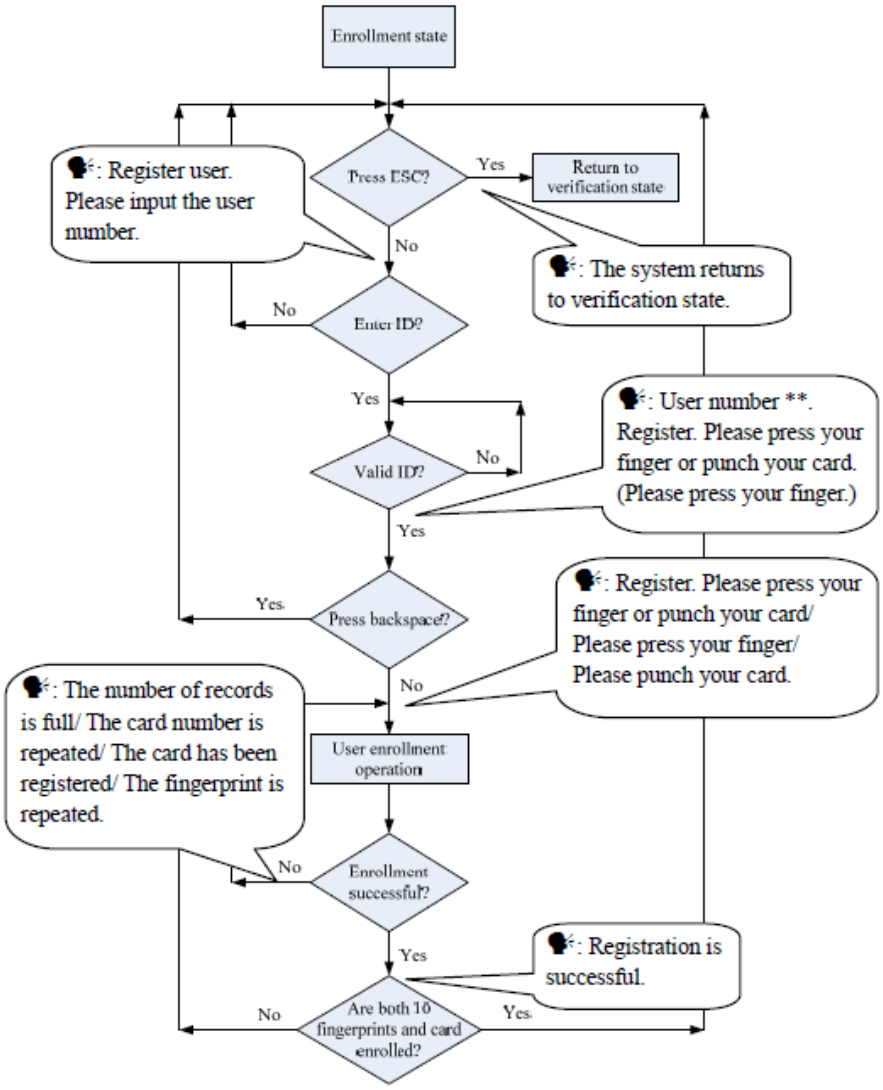
4. El usuario a inscribirse en la operación de identificación del estado de inscripción especificado es similar a la identificación especificada inscribirse operación en el modo de administración de inscripción de tarjetas. Para más detalles, véase el punto 3.1.2 Inscripción de un usuario corriente.

5. En el estado de ID de usuario inscrito en espera, presione la tecla **ESC** *para volver al estado de verificación. En el estado de inscripción especificado por el usuario ID, presione la tecla* **ESC** *dos veces para volver al estado de verificación.*

Nota: *En el modo de inscripción basada en el teclado, se puede inscribir los usuarios en forma consecutiva. Al éxito de inscripción, el sistema regresa automáticamente al estado de la inscripción.*

El teclado basado en diagrama de flujo de inscripción es el siguiente:

www.SEGO.com.pe



Importante declaración:

1. En el modo de inscripción basada en el teclado, en su caso el tiempo de espera de operación, el sistema automáticamente le indicará de esta operación una vez por otros 10 segundos y vuelve al estado de la verificación después de que le pide tres veces.

2. Las huellas dactilares de nuevo ingreso se sobreponen a los originales en el modo de gestión basado en tarjeta de inscripción y el modo de teclado de inscripción basado en lo mismo.

3. Un usuario sólo puede inscribirse una sola tarjeta. Cuando el usuario con una tarjeta de inscripción se inscribe en el sistema, el sistema genera el mensaje de voz : "Registro por favor, presione su dedo. "Cuando el usuario pasa la tarjeta, el sistema genera el mensaje de voz" La tarjeta ha sido registrado. "

4. Una tarjeta no puede ser inscrito repetitiva, de lo contrario el sistema generará el mensaje de voz : "El número de la tarjeta se repite." Durante tarjeta de deslizar. Los diferentes usuarios no se pueden inscribir la misma huella digital, de lo contrario el sistema generará el mensaje de voz :

"La huella digital se repite." Durante el registro de huellas dactilares. Nuevas huellas digitales de un usuario se sobreponen a los ya existentes.

La diferencia entre dos modos de matricula de usuario con respecto al estado de salida de inscripción:

1. En el modo de gestión basado en tarjeta de inscripción con un ID de usuario especificado, el sistema vuelve al estado de la verificación después de que pase su tarjeta una vez.

2. En el modo de inscripción basada en el teclado con un ID de usuario especificado, cuando se presiona la tecla ESC, el sistema vuelve al estado de matrícula y genera el mensaje de voz "registrar a los usuarios. Por favor introduce el número de usuario. "Usted puede inscribir a un ID de usuario y presione la tecla ESC. A continuación, el sistema genera el mensaje de voz "El sistema vuelve al estado de verificación.

3.2.3 Eliminar un usuario especificado

Eliminación de un usuario mediante un teclado externo que se llama el modo de eliminación de usuarios especificado.

Los pasos de la operación:

1. Conecte un teclado USB al dispositivo, y pase su tarjeta de gestión de una o introducir la contraseña para activar el teclado.

2. Pulse la tecla "2" y Enter para entrar en el modo de eliminación de usuarios especificado. El sistema generará el mensaje de voz "Eliminar usuarios. Por favor introduce el número de usuario. "Y usted puede proceder a la Paso 3.

Aviso: *Un caso especial:*

Si no hay ningún usuario (incluye gestión de usuarios de la tarjeta) inscritos, y usted tiene la contraseña del teclado, puede utilizar la contraseña para activar el teclado y pulse 2 y Enter para entrar en el estado de la eliminación del usuario, el sistema generará la indicación de voz "no usuario registrado. El sistema vuelve al estado de verificación. "

3. Introduzca un ID de usuario y el sistema comprueba si el identificador de usuario es válido.

*4. Si el ID de usuario es válido, el sistema generará el mensaje de voz "el número de usuario. ** La eliminación se realiza correctamente. Eliminar usuarios. Por favor introduce el número de usuario. "Y automáticamente volverá al estado de borrado. Si el ID de usuario no es válido, el sistema generará el mensaje de voz "ID de usuario incorrecto."*

5. Si pulsa la tecla ESC o los tiempos de espera de la operación, el sistema volverá al estado de verificación.

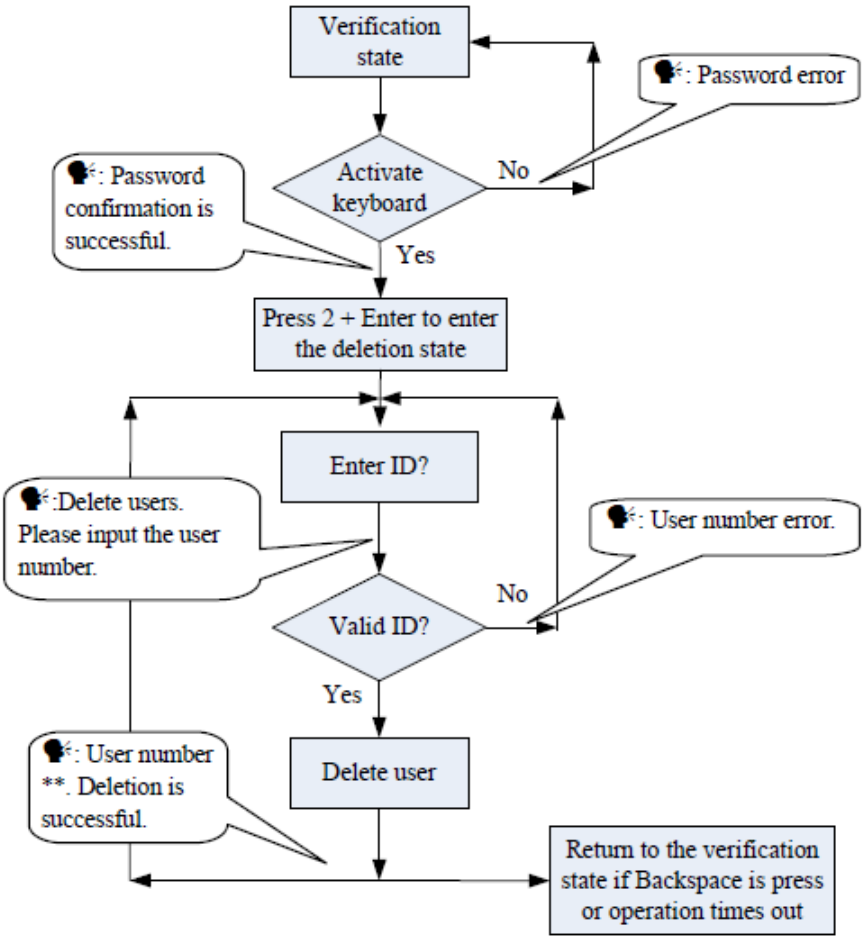
Nota:

www.SEGO.com.pe

1) En el modo especificado eliminación de usuario, ID de usuario y la gestión de las identificaciones de usuario de la tarjeta que están inscritos en el sistema están considerará inválida.

2) En el modo de eliminación basado en el teclado, el sistema de desactivar el sensor de huella digital y lector de tarjetas y por lo tanto, cualquier operación sobre ellos no es válido.

La supresión especificado usuario diagrama de flujo que se muestra a continuación:



3.2.4 Eliminar todos los usuarios

Los pasos de la operación:

1. Conecte un teclado USB al dispositivo, y pase su tarjeta de gestión de una o introducir la contraseña para activar el teclado.

2. Presione "9" y Enter. A continuación, pulse "9" y Enter de nuevo. El sistema borra todos los usuarios.

3. Si la operación tiene éxito, el sistema generará el mensaje de voz: "Eliminar todos los usuarios. La operación se realiza correctamente. El sistema vuelve al estado de verificación. Por

favor, el registro de la tarjeta de gestión".

Nota:
1) Puede eliminar una tarjeta de gestión utilizando la función Eliminar Todos.
2) Se puede utilizar la función Eliminar Todos para borrar todos los usuarios inscritos, huellas dactilares y registros.
3). Extrema precaución debe ser ejercida al realizar esta operación, ya que una vez eliminados, los datos no se pueden recuperar.

3.2.5 Restaurar valores predeterminados de fábrica

Los pasos de la operación:

1. Conecte un teclado USB al dispositivo, y pase su tarjeta de gestión de una o introducir la contraseña para activar el teclado.

2. Pulse "3" y Enter. A continuación, pulse "3" y Enter de nuevo. El sistema restaura los valores predeterminados de fábrica.

3. Después de la operación se realiza correctamente, el sistema genera el mensaje de voz "Restaurar la configuración por defecto. La operación se realiza correctamente. El sistema vuelve al estado de verificación. "

También puede restaurar los valores predeterminados de fábrica al restablecer el interruptor de sabotaje. Ver 3,6 interruptor de sabotaje.

Después de que el dispositivo se restablece a los valores de fábrica, la información del dispositivo se restaura a los valores predeterminados de fábrica, incluyendo el número de dispositivo, contraseña de sistema, dirección IP, la dirección 485, y la contraseña del teclado.

La información de usuario almacenada en el dispositivo no se borrará después de que el dispositivo se restablece a los valores de fábrica.

3.3 Función de Control de Acceso

Marco de control de acceso es configurar el usuario de zona de tiempo de apertura de puertas, cerraduras de control y los parámetros del dispositivo vinculado.

Para desbloquear, el usuario registrado deberá ajustarse a las siguientes condiciones:
1. El tiempo de desbloqueo actual debe estar en el tiempo efectivo de la zona de usuario de tiempo o de la zona de grupo.

2. El grupo donde el usuario es debe estar en el control de acceso (o en el control de acceso mismo con otro grupo, para abrir la puerta juntos).

www.SEGO.com.pe

El sistema por defecto el nuevo inscrito el usuario como el grupo de la primera zona, por defecto el tiempo de grupo como 1, el control de acceso como el primer grupo, y el nuevo usuario inscrito en desbloqueo (El usuario puede modificar la configuración relacionada con el control de acceso, a través del software de control de acceso).

Aviso: *El acceso a los dispositivos de control de la función de la necesidad de establecer y modificar a través del software de control de acceso, para más detalles, consulte el manual de usuario del software.*

Acceder a la función de control:

1. Acceder a la Zona de Control de Tiempo:
La zona horaria es la unidad mínima de la opción de control de acceso. Todo el sistema puede definir 50 zonas horarias. Cada zona horaria define siete secciones de tiempo (es decir, a la semana). Cada intervalo de tiempo es la zona de tiempo efectivo dentro de las 24 horas todos los días. Cada usuario puede establecer 3 zonas horarias. "O" existe entre las tres zonas. Es eficaz si sólo uno está satisfecho.

2. Configurar el acceso de vacaciones:
Un tiempo especial de control de acceso puede ser necesario durante las vacaciones. Es diferente para modificar el tiempo de todos de control de acceso. Así que un día de fiesta el tiempo de acceso de control se puede establecer, que es aplicable para todos los empleados.

3. Grupo de acceder a la Zona de tiempo:
La agrupación es manejar a los empleados en grupos. De los trabajadores en grupos utilizan la zona correspondiente grupo de tiempo por defecto. Los miembros del grupo también se pueden definir la zona de usuario del tiempo. Cada grupo puede tener que las zonas horarias. El nuevo usuario inscrito pertenece al Grupo 1 de forma predeterminada y también pueden ser asignados a otros grupos.

4. Desbloquear Marco de combinación:
Hacer varios grupos en diferentes controles de acceso para lograr multi-verificación y mejorar la seguridad. Un control de acceso puede esta compuesta de 5 grupos a lo sumo.

5. Acceder a los parámetros de control:
Bloqueo de retardo de control: se aplican para determinar horas de desbloqueo, los min medidos unidad 20ms, en la condición normal es de 100-200ms.
Anti-Pass Mode*: Se puede establecer en "Ninguno", "Fuera", "En", "In-Out".*
Estado de registro Maestría: *Se puede establecer en "Ninguno", "Fuera", "En".*
Modo del sensor: *Modo del sensor de puerta. Puede ser configurado en "Ninguno", "NAbrir", "NClose" del Estado.*
Retraso del sensor: *Establecer el tiempo de retardo del sensor cuando se abre la puerta. Después de este tiempo se define el sensor de detectar el estado de puerta. Si el estado de la puerta no es coherente que la alarma se activará. Amplia pantalla del dispositivo en blanco y negro es 0-254. Pantalla a color de gama de equipos es 0-99.*

www.SEGO.com.pe

Alarma Sensor: *Establecer el tiempo de retardo de alarma después de la alarma se dispara. El rango es de 0-999 segundos.*
Tiempos de error a la alarma: *Definir los tiempos de error máximo para activar la alarma. Cuando la verificación no es a través, y superar estos tiempos definidos, la señal de alarma se activará automáticamente.*

6. Anti-pass back configuración:
función Anti-pass back por favor refiérase a 4.2 Anti-Pass back.

7. Desactivar la alarma:
Cuando el dispositivo está en estado de alarma, la verificación del usuario puede desactivar la alarma, y el dispositivo se recuperará estado normal. Si no, se alarma todo el tiempo.
Tipos de alarma: *alarma de la puerta del sensor y alarma de sabotaje.*

3.4 Verificación del usuario
La verificación por defecto del dispositivo es de PF / RF de verificación, el usuario puede utilizar el software de control de acceso para modificar el modo de verificación a la RF, PF o RF y verificación de FP. Para más detalles consulte el manual de usuario del software.
Los pasos de la operación:

1. Cuando el dispositivo está en estado de verificación, el sistema genera el mensaje de voz "Verifique los usuarios. Por favor, pulse el dedo o pase su tarjeta. "

2. Iniciar la verificación del usuario. El dispositivo es compatible con cuatro modos de verificación: PF / RF, FP, RF y verificación de FP y de RF.

(1) la verificación de huellas dactilares
*Presione su dedo en el sensor de huellas digitales de una manera apropiada. Si la verificación tiene éxito, el sistema genera el mensaje de voz "** usuario número. Gracias. "Y al mismo tiempo activa una señal de desbloqueo. Si la verificación falla, el sistema genera el mensaje de voz "Por favor, inténtelo de nuevo"*

(2) verificación de la tarjeta
*Deslice su tarjeta en el lector de tarjetas. Si la verificación tiene éxito, el sistema genera el mensaje de voz "** usuario número. Gracias. " Y al mismo tiempo activa una señal de desbloqueo. Si la verificación falla, el sistema genera el mensaje de voz "Por favor, pase su tarjeta de nuevo"*

(3) Huellas digitales + tarjeta de verificación
Ajuste el modo de verificación del usuario a la PF y RF a través del software de control de acceso, la operación de verificación de la siguiente manera:

Pulse el primer dedo:
*Presione su dedo en el sensor de huellas digitales de una manera apropiada. Si la verificación tiene éxito, el sistema genera el mensaje de voz "el número de usuario **, por favor, pase su tarjeta." Después de la verificación de la tarjeta tenga éxito, y al mismo tiempo activa una señal de*

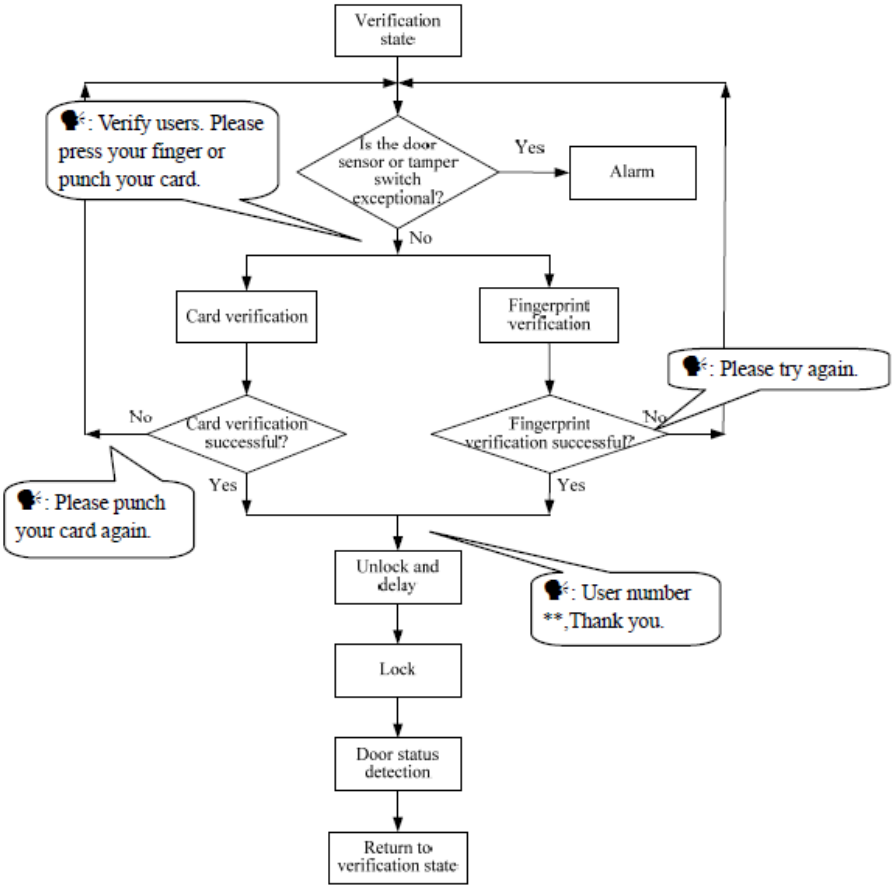
desbloqueo. Si la verificación falla, el sistema genera el mensaje de voz "Por favor, pase su tarjeta de nuevo."

Pase la primera tarjeta:
*Deslice su tarjeta en el lector de tarjetas. Si la verificación tiene éxito, el sistema genera el mensaje de voz "el número de usuario **, por favor presione el dedo." Después de la verificación de huellas dactilares éxito, y al mismo tiempo activa una señal de desbloqueo. Si la verificación falla, el sistema genera el mensaje de voz "Por favor, inténtelo de nuevo."*

(4) Huellas dactilares o tarjeta de verificación

Esto es, la operación de comprobación de (1) o (2) a la vez eficaz.

La verificación del usuario diagrama de flujo se muestran a continuación:



Consejo:
(1) Si el usuario no está en el huso horario el acceso efectivo de control, no puede verificar y abrir la puerta, el sistema genera el mensaje de voz "Zona horaria no válido"

(2) Si el usuario no se utiliza el modo de verificación conjunto para verificar, no se puede verificar y abrir la puerta, el sistema genera el mensaje de voz "Modo de Verificación no válido."

3.5 U-disco

El usuario puede realizar la descarga en disco, descarga del usuario, el usuario carga y actualización de firmware a través de un U-disco.

a. Registro descarga: *Descargar los registros de asistencia de todos los usuarios del dispositivo a un U-disco.*

b. Usuario descarga: *Descargar toda la información del usuario, como las huellas dactilares y números de tarjetas desde el dispositivo a un U-disco.*

c. Usuario: *Transfiera la información de usuario a partir de un U-disco en el dispositivo.*

d. Actualización del firmware: *Actualizar el firmware del dispositivo a través de un U-disco.*
Los archivos de configuración en el U-disco se pueden crear y modificar mediante el software de control de acceso. La operación, por favor consulte el manual de usuario del software.

Aviso: *Por favor no actualice el firmware a su discreción, ya que puede traer problemas y afectar el uso normal del dispositivo. Póngase en contacto con nuestros distribuidores para obtener asistencia técnica o de la notificación de actualización.*

U-disco incluye las operaciones de los dos casos siguientes:
1. Si conecta un U-disco sin archivo de configuración para el dispositivo, el sistema se lo indicará automáticamente de las operaciones en la secuencia.

(1) Después de conectar un U-disco en el dispositivo, se puede deslizar su tarjeta una vez para entrar en el estado de gestión de U-disco.

*(2) El sistema genera el mensaje de voz ". **** Por favor, pase su tarjeta de gestión para su confirmación". (**** Indica que los elementos de operación cuatro de A y D en la secuencia; lo mismo más adelante).*

(3) Si usted desea llevar a cabo la gestión de U-disco, pase su tarjeta para su confirmación. Si la operación tiene éxito, el sistema generará el mensaje de voz "La operación es un éxito." Y le pedirá que continúe con el paso siguiente. Después de terminar los cuatro elementos, el sistema genera el mensaje de voz "El sistema vuelve al estado de verificación." Si la operación falla, el sistema generará el mensaje de voz "la operación falla. El sistema vuelve al estado de verificación."

(4) Si no lo hace pasar la tarjeta de gestión, el sistema automáticamente omitirá este paso en 5 segundos y le pedirá que de el siguiente paso. Después de terminar los cuatro elementos, el sistema vuelve al estado de verificación de forma automática.

2. Si conecta un U-disco con el archivo de configuración para el dispositivo, el sistema llevará a cabo operaciones basadas en la configuración del archivo de configuración.

www.SEGO.com.pe

(1) Después de conectar un U-disco en el dispositivo, se puede deslizar su tarjeta una vez para entrar en el estado de gestión de U-disco.

(2) El sistema obtiene los comandos de la operación mediante la lectura del archivo de configuración en el U-disco y genera el mensaje de voz en "Ejecutar los archivos de configuración en el U-disco. Por favor, pase su tarjeta de gestión para su confirmación."

*(3) Después de pasar la tarjeta y realizar todas las operaciones con éxito, el sistema generará el mensaje de voz "**** La operación se realiza correctamente. "En la secuencia para cada paso de la operación. Si cualquiera de las operaciones falla, el sistema generará el mensaje de voz "****.La operación falla."*

(4) Después de terminar todas las operaciones, el sistema genera el mensaje de voz "El sistema vuelve al estado de verificación."

Aviso: *Por favor, espere 8 segundos después de insertar el U-disco en el dispositivo, de lo contrario, el sistema no puede detectar el U-disco, probablemente.*

3.6 Interruptor de sabotaje

El interruptor de sabotaje se mantiene pulsado con una cubierta trasera. Cuando el dispositivo está desmantelado, el interruptor de sabotaje se levantó y, a continuación, envía una señal de alarma para activar una alarma.
Borrar la alarma: *El usuario puede desactivar la alarma, abrir la puerta en concordancia con éxito.*
Restaurar valores predeterminados de fábrica: *Los valores predeterminados de fábrica se pueden restaurar a través del interruptor de sabotaje.*
Cuando el sistema genera una alarma durante 30-60 segundos, el usuario puede pulsar el interruptor de sabotaje (tres veces hasta que los sonidos de los altavoces) para restaurar la configuración por defecto, incluyendo el número de dispositivo, contraseña de sistema, dirección IP, la dirección 485, y la contraseña del teclado.

Nota:
1. La información de usuario almacenada en el dispositivo no se borrará después de que el dispositivo se restablece a los valores de fábrica.
2. Los valores predeterminados de fábrica se pueden restaurar a través del teclado USB. Para obtener más información, consulte 3.2.5 Restaurar valores predeterminados de fábrica.

4. apéndice

4.1 Lista de parámetros

La siguiente tabla muestra los parámetros básicos de funcionamiento del dispositivo.

www.SEGO.com.pe

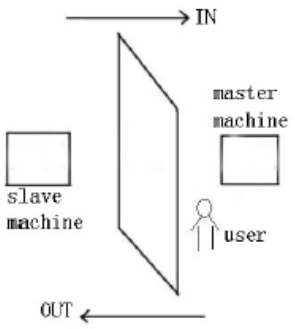
Item	Note
Power Supply	12V 3A
Function	Access control device, door sensor/ alarm/ lock/ exit button
	One Wiegand input and one Wiegand output
User quantity	10000 (fingerprint and ID card)
Record capacity	100000 pieces of records
Enrollment capacity (fingerprint/card)	1500 fingerprints/10000 cards
Verification mode.	ID (Mifare) card, fingerprint, fingerprint + card
Communications	TCP/IP, RS485, U-disk
Speaker	Voice, BEEP
LED	Bi-color indication (red/green)
Keyboard	Valid keys: 0-9, Enter, ESC

4.2 Anti-Pass back ★

[Resumen]

A veces, alguna persona ilegal sigue el otro en la puerta, que traerá problema de seguridad. Para evitar este riesgo, esta función está activada. En el registro deben coincidir con registro, o la puerta no se abrirá.

Esta función necesita dos máquinas para trabajar juntos. Uno se instala dentro de la pista (en lo sucesivo maestro de la máquina), el otro está instalado fuera de la pista (en lo sucesivo esclavo de la máquina). La comunicación Wiegand señal de que se adopte entre las dos máquinas.



[Principio de funcionamiento] *La máquina maestra ha Wiegand de esclavos y la máquina ha Wiegand de salida. Conecte Wiegand de salida de la máquina esclavo de Wiegand en la máquina principal. Wiegand de salida de la máquina esclava no debe poseer identificación de la máquina. El número enviado a dominar máquina de la máquina esclavo se debe encontrar en la máquina maestra.*

[Función]

www.SEGO.com.pe

juzgar si es anti-pass back, según un reciente usuario en todo el registro. En el registro y la salida debe ser igualado apoya a cabo, dentro o fuera en la lucha contra el pase hacia atrás.

Cuando la máquina principal se configura como "fuera contra el pasar de nuevo", si el usuario quiere entrar y salir con normalidad, su reciente disco debe estar "en", o que no pueden salir. Cualquier "salida" disco va a ser "anti-pasar de nuevo se negó". Por ejemplo, el historial reciente de un usuario es "in", su segundo disco puede estar "fuera" o "en". Su tercer disco se basa en su segundo disco. Fuera de registro y en el registro debe coincidir con (aviso: si el cliente no tiene ningún registro antes, entonces él puede entrar, pero no se puede salir).
Cuando la máquina principal se establece como "en la lucha contra el pase hacia atrás, si el usuario quiere entrar y salir disco va a ser" anti-pass back se negó "por el sistema (nota: si el cliente no tiene ningún registro anterior, entonces él puede salir, pero no puede entrar). Cuando la máquina principal se configura como "out-in anti-pasar de nuevo", si el usuario quiere entrar y salir normalmente, si su reciente disco es "fuera" y "en", entonces su próximo disco debe estar "en "y" fuera".

[Operación]
1. seleccione el modelo
máquina maestra: *la máquina con Wiegand en la función, a excepción de F10 lector.*
Máquina esclava: *la máquina con la función de Salida Wiegand.*
2. establece anti-pass dirección hacia atrás y el estado del dispositivo.
3. modificar el formato del dispositivo de salida Wiegand
cuando los dos dispositivos se comunican, sólo las señales de identificación del dispositivo Wiegand, sin que se reciban.
4. inscripción del usuario
el usuario debe ser en la máquina de maestro y esclavo de la máquina al mismo tiempo, y el PIN usuario debe ser el mismo. por lo tanto, si es necesario para inscribirse usuario en la máquina de maestro y esclavo de la máquina al mismo tiempo.

www.SEGO.com.pe